# Redacted



**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN JOSE DIVISION**

FINJAN, INC.,

Plaintiff,

v.

CISCO SYSTEMS INC.,

Defendant.

Case No. 17-cv-00072-BLF

**ORDER GRANTING IN PART AND DENYING IN PART CISCO'S MOTION FOR PARTIAL SUMMARY JUDGMENT OF NON-INFRINGEMENT**

[Re: ECF 378]

Plaintiff Finjan, Inc. ("Finjan") brings this patent infringement lawsuit against Defendant Cisco Systems, Inc. ("Cisco"), alleging infringement of five of Finjan's patents directed to computer and network security: U.S. Patent Nos. 6,154,844 (the "'844 Patent"); 6,804,780 (the "'780 patent"); 7,647,633 (the "'633 patent"); 8,141,154 (the "'154 patent"); and 8,677,494 (the "'494 patent"). Cisco seeks summary judgment of non-infringement on 3 of the 5 asserted patents: the '154 Patent, the '633 Patent, and the '780 Patent. Cisco also seeks summary judgment of no pre-suit damages. The Court heard oral arguments on January 9, 2020 (the "Hearing").

## I. THE ACCUSED PRODUCTS

The infringement allegations subject to Cisco's motion for summary judgment primarily relate to Cisco's Advanced Malware Protection ("AMP") products under the following categories: (1) AMP Gateway/Cloud Products (for Enterprise) and AMP for Endpoints (collectively, "AMP Products") and (2) Talos (or its component, [redacted] and Threat Grid (collectively "Cisco Sandboxes"). Cisco Systems, Inc.'s Motion for Partial Summary Judgment ("MSJ") at 1, ECF 382-3 (redacted version filed at ECF 378); Plaintiff Finjan, Inc.'s Opposition to Defendant Cisco Systems, Inc.'s Motion for Partial Summary Judgment ("Opp'n") at 1-2, ECF 400-4 (redacted version filed at ECF 401). The AMP Products screen incoming files that are intended for a user's

device for malicious content. MSJ at 1.

For the AMP Gateway Products, a requested file is processed as follows: [redacted] MSJ at 2. The AMP appliance may also send a copy of an unknown file to Cisco's "sandboxes," known as Threat Grid and [redacted] *Id.* AMP for Endpoints operates similarly to AMP Gateway, except it runs on client (end-user) devices instead of running at a gateway. *Id.*

Finjan also accuses the "URL rewriting" feature within the Cisco E-mail Security Appliance ("ESA") with respect to the '154 Patent only. MSJ at 2; Opp'n at 2. Cisco's ESA products screen incoming emails for malicious content before they are delivered to a user's inbox.

## II. LEGAL STANDARD

Federal Rule of Civil Procedure 56 governs motions for summary judgment. Summary judgment is appropriate if the evidence and all reasonable inferences in the light most favorable to the nonmoving party "show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). Rule 56 authorizes a court to grant "partial summary judgment" to dispose of less than the entire case and even just portions of a claim or defense. *See* Fed. R. Civ. P. advisory committee's note, 2010 amendments.

The moving party bears the burden of showing there is no material factual dispute, by "identifying for the court the portions of the materials on file that it believes demonstrate the absence of any genuine issue of material fact." *T.W. Elec. Serv. Inc. v. Pac. Elec. Contractors Ass'n*, 809 F.2d 626, 630 (9th Cir. 1987). In judging evidence at the summary judgment stage, the Court "does not assess credibility or weigh the evidence, but simply determines whether there is a genuine factual issue for trial." *House v. Bell*, 547 U.S. 518, 559-60 (2006). A fact is "material" if it "might affect the outcome of the suit under the governing law," and a dispute as to a material fact is "genuine" if

there is sufficient evidence for a reasonable trier of fact to decide in favor of the nonmoving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986).

In cases like this, where the nonmoving party will bear the burden of proof at trial on a dispositive issue (*e.g.*, patent infringement), the nonmoving party must "go beyond the pleadings and by her own affidavits, or by the 'depositions, answers to interrogatories, and admissions on file,' designate 'specific facts showing that there is a genuine issue for trial.'" *Celotex*, 477 U.S. at 324. For a court to find that a genuine dispute of material fact exists, "there must be enough doubt for a reasonable trier of fact to find for the [non-moving party]." *Corales v. Bennett*, 567 F.3d 554, 562 (9th Cir. 2009). In considering all motions for summary judgment, "[t]he evidence of the non-movant is to be believed, and all justifiable inferences are to be drawn in his favor." *Anderson*, 477 U.S. at 255; *see also Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986).

## III. DISCUSSION

### A. The Parties' Dispute Regarding Finjan's Expert Reports on Infringement

As an initial matter, the Court addresses a procedural dispute regarding Finjan's expert reports on infringement. Finjan's infringement theories in this case have been the subject of extensive motion practice. On April 18, 2019, Finjan moved to supplement (or amend) its infringement contentions pursuant to Local Patent Rule 3-6. ECF 231. On June 11, 2019, Magistrate Judge van Keulen denied Finjan's motion and rejected its assertion that it was simply adding the codenames of particular components to its previous contentions regarding the associated functionality. ECF 274 at 6-7. Finjan sought relief from Judge van Keulen's order, which this Court denied on July 17, 2019. ECF 304 at 3-4. Finjan served its expert infringement reports – which included the codenames in dispute – and Cisco moved to strike. ECF 312. The Court granted Cisco's motion and directed Finjan's experts to "redraft their reports to remove the disallowed terminology and Talos-only allegations, and to ensure that their opinions track the disclosures in Finjan's operative infringement contentions." ECF 397 at 7. At the Hearing, the parties informed the Court that they had not yet finalized the revised infringement expert reports. *See* Transcript of Proceedings Before the Honorable Beth Labson Freeman on January 9, 2020 ("Hr'g Tr.") at 49:18-50:21, ECF 419.

As a result, the basis for Cisco's present motion for summary judgment is Finjan's now-stricken expert reports that include the disallowed codenames. In several instances, Cisco seeks summary judgment on the ground that that the accused codenames have been stricken and thus, cannot be relied upon to show infringement. The Court rejects those arguments wholesale without prejudice. As the Court explained at the Hearing, the Court struck certain codenames from Finjan's expert reports – but not the experts' opinions generally. Hr'g Tr. at 50:22-51:6. The Court further allowed Finjan to amend its reports and substitute the disallowed codenames with functionalities that were included in Finjan's infringement contentions. As of the date of this Order, the Court is not aware of any amended expert reports. Accordingly, the Court decides on Cisco's motion for summary judgment under the assumption that the codenames used in the expert reports (and the parties' briefing) have a corresponding functionality in the infringement contentions and thus, are still in the case. If, however, Finjan is unable to show that the functionalities corresponding to the codenames were included in its operating infringement contentions, the Court would entertain that dispute in a motion *in limine*. *See* Hr'g Tr. at 159:14-17.

**B. Non-infringement of the '154 Patent**

**1. Background of the '154 Patent**

The '154 patent is directed to a system and a method "for protecting a client computer from dynamically generated malicious content[.]" '154 Patent at Abstract. Conventional reactive anti-virus applications perform file scans looking for a virus's signature against a list known virus signatures kept on a signature file and thus, cannot protect against first time viruses or if a user's signature file is out of date. '154 Patent at 1:25-31, *id.* at 2:32-37. Proactive anti-virus application, on the other hand, use "a methodology known as 'behavioral analysis' to analyze computer content for the presence of viruses." *Id.* at 1:56-58.

Dynamic virus generation occurs at runtime where dynamically generated HTML contains malicious JavaScript code. '154 Patent at 3:53-64. For example the JavaScript function document.write() is used to generate dynamic HTML at runtime. *Id.* at 3:53-57. Malicious code inserted in a document.write() function would not be caught prior to runtime because the malicious code is not present in the content prior to runtime. *Id.* at 3:65-4:4. To this point, the '154 Patent

concerns a "new behavioral analysis technology [that] affords protection against dynamically generated malicious code, in addition to conventional computer viruses that are statically generated." *Id.* at 4:31-34.

The basic setup of the '154 Patent involves three components: (1) gateway computer including a content modifier, (2) client computer including a content processor, and (3) security computer including an inspector, a database of client security policies, and an input modifier. '154 Patent at 9:5-11. A preferred embodiment describes a gateway computer that receives content including a call to an original function and an input. *Id.* at 5:6-9. The gateway computer then substitutes the call to the original function with a corresponding call to a substitute function, which operates to send the input to a security computer for inspection. *Id.* at 5:10-15. The gateway computer transmits the "modified content from the gateway computer to the client computer, processing the modified content at the client computer." *Id.* at 5:13-15. The client computer then transmits "the input to the security computer for inspection when the substitute function is invoked." *Id.* at 5:15-17. The security computer first determines "whether it is safe for the client computer to invoke the original function with the input." *Id.* at 5:17-19. The security computer then transmits "an indicator of whether it is safe for the client computer to invoke the original function with the input," to the client computer. *Id.* at 5:19-22. The client computer invokes the original function "only if the indicator received from the security computer indicates that such invocation is safe." *Id.* at 5:22-24.

Claim 1 (the only asserted independent claim of the '154 Patent) provides:

> A system for protecting a computer from dynamically generated malicious content, comprising:
>
> > a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe;
> >
> > a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and
> >
> > a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with

the input.

'154 patent, 17:32-44.

The Court construed "first function / second function" as "substitute function / original function, which is different than the first function." Order Construing Claims in U.S. Patent Nos. 6,154,844; 6,804,780; 7,647,633; 8,141,154; 8,677,494 ("*Markman* Order I") at 35, ECF 134.

**2. AMP Products**

The non-infringement dispute raised in Cisco's motion for summary judgment is centered on whether the AMP Products satisfy the claimed "content" that includes a "call to a first [*i.e.*, substitute] function" as construed by the Court.[1] Cisco argues that it is entitled to summary judgment as to the accused AMP Products because "AMP does not substitute calls to functions into any content that it receives." MSJ at 5. According to Cisco, (1) [redacted] 2) [redacted] *Id.* at 5-6. Under Finjan's infringement analysis, Cisco argues, "both the 'substitute function' and the 'original function' can exist within the content as it was originally created," which in turn "renders the word 'substitute' meaningless." *Id.* at 6.

Finjan responds that claim 1, under the Court's claim construction, does "not require that the system have a gateway or a content modifier." Opp'n at 3. Relying on that premise, Finjan argues that it has demonstrated that there is a "substitute" function (or first function) which is different from the "second function." *Id.* The allegedly infringing example that Finjan provides is that "there are scenarios where the hacker or some other process modifies the original content by inserting a substitute function in place of the original function." *Id.* (citing Expert Report of Michael Mitzenmacher, Ph.D. Regarding Infringement by Cisco Systems, Inc. of Patent Nos. 6,804,780 and

[1] In its moving papers, Cisco argued that Finjan's infringement expert, Dr. Mitzenmacher, relied on an incorrect interpretation of the Court's claim construction. MSJ at 4-5. As the briefing progressed, however, it appears that the parties no longer present a claim construction dispute. *See* Opp'n at 4, Reply at 2, Hr'g Tr. at 57:1-20, ECF 419. Thus, the Court need not address this argument.

8,141,154 ("Mitz. Rpt") ¶ 1934, ECF 400-6). At the Hearing, Finjan provided the same example. *See* Hr'g Tr. at 59:19-25.

The Court is not persuaded by Finjan's arguments because they are inconsistent with the patent's specification and the Court's *Markman* Order. Under Finjan's theory, the "substitute function" can be supplied by an external actor (*e.g.*, a hacker) outside the control of any accused product. *See* Hr'g Tr. at 63:13-18. This theory is contrary to how the '154 Patent describes the invention. According to the '154 Patent's own language:

> To enable the client computer to pass function inputs to the security computer and suspend processing of content pending replies from the security computer, ***the present invention operates by replacing original function calls with substitute function calls within the content, at a gateway computer, prior to the content being received at the client computer***.

'154 Patent at 4:55-60 (emphasis added). It is the "invention" that replaces the "original" function with a "substitute" function – not an external factor such as a hacker. As Judge Alsup explained in Finjan's case against Juniper, a "substitute function" supplied by an external system "ultimately amounts to the original content initially received by the claimed system" and not a "substitute" function. *Finjan, Inc. v. Juniper Networks, Inc.*, No. C 17-05659 WHA, 2019 WL 3302717, at *2 (N.D. Cal. July 23, 2019).

Finjan's "hacker" theory is also inconsistent with the Court's construction of "first function/second function." It is true that claim 1 does not recite or claim a "gateway that modifies content." *See Markman* Order I at 38. But, in construing "first function" to mean "substitute function," the Court acknowledged that the content received by the "content processor" includes a call to "substitute function" — which replaced the "original function" at the (unclaimed) gateway. *See Markman* Order I at 38 ("[T]he specification clearly discloses a content modifier in the gateway that modifies original content to replace the original function with the substitute function.") (citing '154 Patent at 9:13–28). The Court explained that "a person of ordinary skill in the art would understand that the 'first function' corresponds to the substitute function in light of the claim language and the specification." *Markman* Order at 38. Thus, the Court's claim construction

requires the "original function" be replaced by the "substitute function."[2] To hold otherwise, renders the word "substitute" in the Court's construction meaningless.

To support its position, Cisco cites to Judge Alsup's decision in Finjan's case against Juniper, finding that the "the substitute function exists only after the original content is modified at the gateway computer." *Finjan, Inc. v. Juniper Networks, Inc.*, 387 F. Supp. 3d 1004, 1011 (N.D. Cal. 2019) (citing '154 Patent at 9:13–28). To be clear, Judge Alsup was tasked with construing the term "content processor" – which this Court had no occasion to construe. *See id.* at 1010-13. That said, the Court finds Judge Alsup's analysis well-reasoned and supported by the '154 Patent's specification explaining that "the present invention operates by replacing original function calls with substitute function calls within the content, at a gateway computer, prior to the content being received at the client computer." '154 Patent at 4:55-60.

In addition, the Court finds Finjan's "hacker" theory contrary to the Federal Circuit's understanding of claim 1. The Federal Circuit explained:

> The '154 patent has four independent claims (1, 4, 6, and 10), each reciting a system or software program that executes a substitute function. The substitute function inspects the input to an original function to determine if executing the original function with the input violates a security policy.
> …
> In the language of the '154 patent, the "first function" is the inspection step in which the content is assessed for safety, and the "second function" is when, having been deemed safe, the content is actually run.

*Palo Alto Networks, Inc. v. Finjan, Inc.*, 752 F. App'x 1017, 1018 (Fed. Cir. 2018). The Court is not persuaded that a hacker's code "inspects the input" to "determine if executing the original function with the input violates a security policy" or operate as "the inspection step." *See id.*[3] In sum, the Court finds that Finjan's "hacker" infringement theory fails to meet the requirements of

[2] The Court notes that in its case against Proofpoint, Finjan made such an argument to address claim construction of the same disputed term (*i.e.*, first function/second function). *See Finjan, Inc., v. Proofpoint*, Inc., No. 13-CV-05808-HSG, 2015 WL 7770208, at *8 (N.D. Cal. Dec. 3, 2015) ("Plaintiff notes that . . . the original function is replaced by the substitute function at the gateway, *before* the security computer receives the content.") (emphasis in original).

[3] The Court notes that Judge Alsup similarly rejected Finjan's "hacker" theory. *See Finjan, Inc. v. Juniper Networks, Inc.*, 2019 WL 3302717, at *2.

claim 1.

Next, Finjan asserts that there are other disputed issues of fact that preclude summary judgment. Opp'n at 5. The Court addresses and rejects each purported dispute below.

First, Finjan argues that "Cisco's non-infringement arguments for the AMP Products only address when the AMP Cloud is the identified security computer, such that Cisco is not seeking summary disposition for AMP Products in combination with Threat Grid and [redacted] and when they are the security computer." Opp'n at 4-5. Cisco responds that it, in fact, "seeks summary judgment on all accused products, and the identity of the 'security computer' is irrelevant to the issues" because "the AMP Products never receive 'content' with a call to a substitute function" – irrespective of what Finjan accuses as the "security computer." Cisco Systems, Inc.'s Reply in Support of Its Motion for Partial Summary Judgment ("Reply") at 1, ECF 407-3 (redacted version filed at ECF 408). The Court agrees with Cisco. As discussed above, Finjan has not identified "content" including "a call to a substitute function" in the AMP Products – making the identity of the security computer irrelevant.

Second, Finjan claims that Cisco's declarants[4] and Finjan's expert disagree as to whether AMP Products substitute functions. Without explaining ***how*** Dr. Mitzenmacher's cited examples show that AMP "substitutes calls into the content that it receives," Finjan string cites to several paragraphs in Dr. Mitzenmacher's expert report and his deposition transcript. *See* Opp'n at 5 (citing Mitz. Rpt ¶¶ 1678, 1917, 1919, 2001-2004; see also Ex. 3, 8/30/19 Mitz. Tr. at 110:21-111:13). Cisco replies that "those paragraphs do not explain how a call to any function was substituted into the content, nor how any such call results in transmitting an input to a security computer for inspection, and ¶¶1917 and 1919 do not even relate to AMP." Reply at 3. The Court agrees with

[4] In support of its motion for summary judgment, Cisco relies on declarations from 8 of its employees, describing the operation and features of Cisco's products. *See* ECF 382-11, ECF 382-13, ECF 382-15, ECF 382-17, ECF 382-19, ECF 382-21, ECF 382-23, ECF 382-25. Finjan criticizes Cisco's reliance on those fact declarations because the declarants "did not appear to have read or understood the '154 Patent and the Court's Claim Construction[.]" Opp'n at 5. Cisco responds that the declarations simply cover "product operation [that] is undisputed in all material respects." Reply at 1. The Court is not aware of any authority (and Finjan has not cited to any) that would prohibit Cisco from relying on fact witnesses' testimony regarding the operation of its products – and thus, rejects Finjan's complaints regarding the employee declarations.

Cisco. Paragraphs 1917 and 1919 of Dr. Mitzenmacher's report discuss Cisco's ESA with Outbreak Filters and not AMP Products. *See* Mitz. Rpt ¶¶ 1917, 1919. The remaining cited paragraphs simply name various features as "substitute function" but fail to describe (and so does Finjan in its Opposition brief) how AMP Products do any sort of substitution. *See* Mitz. Rpt ¶¶ 1678, 2001-2004. As for Dr. Mitzenmacher's deposition testimony, he testified:

> Q. Do you think -- let me strike that. Is it your opinion that a Cisco product reading content could insert a function into the content?
> …
> A. I'm not exactly clear what you're meaning, but in the manner I described, like, it is, you know, changing the interpretation of a function to do something other than what the function would be doing without the Cisco product.
> So it's inserting something in the process somewhere, so I would view that as a -- a change in the interpretation of the content.

Transcript of Videotaped Deposition of Michael Mitzenmacher Ph.D. ("Mitz. Dep.") at 111:14-25, ECF 400-10. Finjan fails to explain how and why Dr. Mitzenmacher's testimony regarding "change in the interpretation of the content" means that AMP Products substitute calls into the content they receive. Finjan relies on an implausible inference from Dr. Mitzenmacher's testimony that it fails to explain in sufficient detail for the Court to credit its argument.

Third, Finjan argues that "Dr. Mitzenmacher provides examples of first functions that the AMP Products receive." Opp'n at 5 (citing Mitz. Rpt ¶¶ 1934-1947, 1966, 1996-98, 2042, 2046-47). Cisco replies that "none of those paragraphs explain how a call to any of the functions he identifies was substituted into the content, much less how it would result in transmitting an input to a security computer for inspection, when invoked." Reply at 3. Again, the Court agrees with Cisco. First, to the extent the string cited paragraphs relate to Finjan's theory that a hacker (or other malicious content) provides the substitute function, the Court has rejected that theory. The remaining paragraphs appear to discuss generally the AMP Products receiving "a call to a first function" but do not explain how the AMP Products supply the "substitute function." *See* Mitz. Rpt ¶¶ 1966, 1996-98, 2042, 2046-47.

Fourth, Finjan argues that there is material dispute as to whether AMP Products ***only*** send hash values to the AMP Cloud – as opposed to other inputs such as URLs. Opp'n at 5 (citing Mitz. Rpt ¶¶ 2043-45). Cisco replies that "[w]hatever the 'AMP Cloud receive[s]' does not impact

whether a substitute function call in the received content sends the input to the AMP Cloud when invoked, which is the issue." Reply at 3. The Court agrees. The issue is whether the AMP products receive content including a call to a "substitute function" as construed by the Court – not the type of content AMP receives.

***

Accordingly, the Court finds that Finjan has failed to identify any material disputed facts as to the AMP Products. Cisco's Motion for Summary Judgment is GRANTED with respect to non-infringement of the asserted claims of the '154 Patent by AMP Products.

**3. Email Security Appliance**

**a. URL Rewriting**

Uniform resource locator ("URL") rewriting is a feature of Cisco's Outbreak Filters, available on Cisco's ESA or Cloud Email Security ("CES"). MSJ at 8; *see also* Mitz. Rpt ¶ 2130. The parties do not dispute the overall functionality of URL rewriting – when Outbreak Filters receive an incoming email, they may "rewrite" a URL within the received email, where the rewritten URL includes an additional address to a Cisco proxy server. Declaration of Don Owens in Support of Cisco Systems, Inc.'s Motion for Partial Summary Judgment ("Owens Decl.") ¶¶ 4, 6-7, ECF 382-21; Mitz. Rpt ¶ 2130. Once the user clicks on the rewritten URL, the user's request will flow through the proxy server and be evaluated for potentially malicious content. Owens Decl. ¶¶ 8, 10-12; Mitz. Rpt ¶ 2130; *see also* Hr'g Tr. at 72:9-15.

Cisco acknowledges that Finjan "identifies some sort of 'substitution'" as to the URL rewriting feature – namely, the rewritten URL is a substitute for the original URL. MSJ at 7. Still, Cisco argues that Finjan's infringement theories fail because "Finjan cannot satisfy the requirements of claim 1 that the 'incoming content' have (i) a call to a first function, (ii) a second function (which is different than the first function), and (iii) an 'input' that is the same for both." *Id.* According to Cisco, Finjan's infringement theory amounts to the original URL (*e.g.*, cnn.com) corresponding to "original function," and "input to the original function" – while the rewritten URL must satisfy both the "substitute function" and "the call to the substitute function." *Id.* at 7-8. Moreover, Cisco argues that a URL is simply an address and thus, is neither a function nor a call to a function. *Id.* at 8.

Finjan responds that its expert "identified a mountain of evidence demonstrating that Cisco's ESA receives content with a call to a first (substitute) function, which complies with the Court's claim construction." Opp'n at 7 (citing Mitz. Rpt at ¶¶ 2115-2214). Specifically, Finjan identifies (1) emails as received "content", (2) the processing of the rewritten URL as "call to first function", (3) URL address to the original content (*e.g.*, cnn.com) as "input" sent to the security computer, and (4) the call to "http://" which calls a "GET" function to process a URL address as the "original function" invoked when the security computer determines that the input is safe. Opp'n at 7 (citing Mitz. Rpt ¶¶ 2130, 2122, 2311, 2335, 2340, 2347-48, 2154). Finjan further argues that Cisco "confuses and conflates the original URL address (*i.e.*, youtube.com) with a call to process the rewritten function (http://secure-web.cisco.com/auth=)." Opp'n at 8. According to Finjan, the latter "calls functionality on the identified security computer to perform an authentication and provide a response."

The Court finds that the parties' dispute concerning the manner in which Cisco's URL rewriting feature utilizes URL functionality precludes summary judgment. Specifically, the parties dispute whether a URL (or a portion thereof) can be a "function," or a "call to function" – with Cisco arguing that URLs are nothing more than addresses and Finjan responding that the processing of a URL can be a function. Rendering all inferences in Finjan's favor, a reasonable jury could find that "http://" (calling a GET function) satisfies the "original function" claimed because it is invoked when the security computer determines that the input (original URL such as cnn.com) is safe or that the processing of the rewritten URL is a "call to first function." *Id.*

***

Cisco's motion for summary judgment is accordingly DENIED with respect to the non-infringement of the asserted claims of the '154 Patent by the URL rewriting feature of the ESA Outbreak Filters.

**b.** [redacted]

Next, Cisco challenges Finjan's theory that [redacted] proxy servers are the claimed "content processors." MSJ at 10-11. Cisco argues that [redacted] "do not receive any content including the rewritten URL" and "neither [redacted] accesses the Internet to retrieve the

resource identified by the original URL." *Id.* at 11 (citing Owens Decl. ¶¶ 8, 10, 11). Finjan disagrees and argues that [redacted] "must, by definition, receive content" because they receive the rewritten URL and the rewritten URL is "content" received by Cisco's ESA. Opp'n at 11. Finjan further argues that because "[redacted] must receive content in some form in order to receive the URLs," Cisco's argument on "whether [redacted] receive email streams directly is beside the point." *Id.* Cisco replies that Finjan contradicts itself because it has identified "emails" as the received "content" but now claims that the rewritten URL itself is the "content." Reply at 6.

The Court agrees with Cisco. In its infringement theory as to Cisco's ESA, Finjan has identified "email" as the "content" received by the content processor. *See* Opp'n at 7 ("Cisco's ESA offerings infringes the '154 Patent because they receive content (***which for the ESA are emails***) ….") (emphasis added), *see also* Hr'g Tr. at 72:6-7. The claim requires "a content processor (i) for processing content received over a network, the content …," meaning the content processor must receive the "content", which in this scenario is "email" – not the rewritten URL and not "content in some form" as Finjan now argues. *See* Opp'n at 11. The Court concludes that Finjan has failed to demonstrate that [redacted] receive "content" (*i.e.*, email) and therefore GRANTS Cisco's motion for summary judgment of non-infringement as to [redacted] accused as "content processors."

### C. Non-infringement of the '633 Patent

#### 1. Background of the '633 Patent

The '633 Patent is directed to a system and method "for protecting network-connectable devices from undesirable downloadable operation." '633 Patent at 1:30-33. The specification explains that conventional virus protection programs fail to protect against certain types of viruses. *Id.* at 1:58-59. These include Downloadable information comprising program code that can include distributable components (*e.g.*, Java applets, JavaScript scripts, ActiveX controls, Visual Basic add-ins, or others) or application components (*e.g.*, Application programs, Trojan horses, or multiple compressed program). *Id.* at 1:60-66. To that end, the '633 Patent "provides protection systems and methods capable of protecting a personal computer . . . from harmful, undesirable, suspicious or other 'malicious' operations that might otherwise be effectuated by remotely operable code." *Id.*

at 2:20-25.

In one embodiment of the invention, one or more "servers" (*e.g.*, firewalls, resources, gateways, email relays or other devices/processes that are capable of receiving and transferring a Downloadable) determine whether the received information includes executable code (and is a "Downloadable"). '633 Patent at 2:39-44. The servers can then deliver "static, configurable and/or extensible remotely operable protection policies to a Downloadable-destination, more typically as a sandboxed package including [a] mobile protection code, downloadable policies and one or more received Downloadables." *Id.* at 2:45-49. Once the mobile protection code is received, it can be executed within the Downloadable-destination "in a manner that enables various Downloadable operations to be detected, intercepted or further responded to via protection operations." *Id.* at 2:49-55.

Claim 14, the only asserted claim of the '633 Patent[5], provides:

> 14. A computer program product, comprising a computer usable medium having a computer readable program code therein, the computer readable program code adapted to be executed for computer security, the method comprising:
>
> providing a system, wherein the system comprises distinct software modules, and wherein the distinct software modules comprise an information re-communicator and a mobile code executor;
>
> receiving, at the information re-communicator, downloadable-information including executable code; and
>
> **causing mobile protection code to be executed by the mobile code executor at a downloadable-information destination such that one or more operations of the executable code at the destination, if attempted, will be processed by the mobile protection code.**

Claim 14, '633 Patent (disputed element bolded).

**2. The Requirements of the Claimed Mobile Protection Code ("MPC")**

The dispute at summary judgment is limited to the Cisco items Finjan has identified as MPC (namely: [redacted]

[5] At the time Cisco filed its motion for summary judgment, claims 1, 8, and 13 of the '633 Patent were also asserted. Per the parties' later stipulation, however, Finjan no longer asserts claims 1, 8 and 13. *See* ECF 388.

[redacted]" – all components of Threat Grid and [redacted] MSJ at 15; Opp'n at 14.[6]

Cisco argues that claim 14 requires an MPC that "(1) is transmitted; (2) is executable; and (3) monitors or intercepts code operations" – and none of the accused products identified by Finjan's expert satisfies all three requirements. MSJ at 11, 15-16. Finjan does not contest the latter two requirements, but responds that "Claim 14 of the '633 Patent has no explicit requirement that MPC be 'transmitted' or 'communicated' with the downloadable-information." Opp'n at 12. At the Hearing, Finjan clarified its position and explained: (1) claim 14 does not require transmission and (2) even if it did, installation of software satisfies that element. Hr'g Tr. at 100:20-24. Finjan further argues that all products accused as MPC meet the claim requirements.

Neither the language of claim 14 nor the Court's construction of MPC requires MPC to be transmitted. First, there can be no dispute that "transmission" does not appear in claim 14. Other claims of the '633 Patent, notably, claims 1, 8, and 13 – which are no longer asserted in this case – require MPC to be transmitted or communicated. *See* '633 Patent, Claim 1 ("… ***transmitting*** from the computer mobile protection code to at least one information destination of the downloadable-information, …") (emphasis added); *id.*, Claim 8 ("… for causing mobile protection code ('MPC') ***to be communicated*** by the computer …"); *id.*, Claim 13 ("…means for causing mobile protection code ***to be communicated*** to at least one information-destination …") (emphasis added). Claim 14 contains no such language, leading to the presumption that its scope differs from that of claims 1, 8 and 13. *See Curtiss-Wright Flow Control Corp. v. Velan, Inc.*, 438 F.3d 1374, 1380 (Fed. Cir. 2006) (recognizing the "presumption that each claim in a patent has a different scope").

Second, the Court construed "mobile protection code" as "code that, at runtime, monitors or

[6] In its opening brief, Cisco also challenged Finjan's theory as to AMP Gateway Products transmitting MPC to Cisco sandbox using APIs. *See* MSJ 13-14. Cisco argued that [redacted] and API calls are not MPC because they are not executable. MSJ at 14. Finjan responds that it "disagrees with Cisco's arguments regarding APIs" but nonetheless, those arguments are "irrelevant because Finjan has not identified RESTful APIs as MPC[.]" Opp'n at 13. Because the parties appear to not dispute this issue, the Court need not address Cisco's arguments regarding APIs.

intercepts actually or potentially malicious code operations without modifying the executable code, where the mobile protection code itself must be executable." *See* Order Granting Cisco's Motion for Reconsideration of the Court's Order Construing Additional Claims at 1, ECF 247. Specifically, the Court rejected Cisco's request to include the term "mobile" in the construction. *See* Order Construing Additional Claims in U.S. Patent Nos. 6,154,844; 6,804,780; 7,647,633 ("*Markman* Order II") at 4-6, ECF 173. Thus, to the extent Cisco asserts that the term "mobile" in "mobile protection code" requires the MPC to be transmitted, the Court's construction imposes no such requirement.

Cisco relies on Finjan's arguments at claim construction and this Court's order in Finjan's case against Blue Coat (where the Court construed a related term) to argue that claim 14 requires "some form of communication" – which pre-installation of software cannot satisfy. *See* Hr'g Tr. at 114:4-6; MSJ at 13; *see also Finjan, Inc. v. Blue Coat Sys.*, Inc., No. 13-CV-03999-BLF, 2014 WL 5361976, at *5 (N.D. Cal. Oct. 20, 2014). The Court is not persuaded. First, the Court carefully considered the parties' arguments at claim construction and elected not to include the term "mobile" (let alone, "transmitted" or "communicated") in the construction of MPC and sees no reason to revisit or modify its construction. *See Markman* Order II at 4-6. Second, one of the embodiments described in the '633 Patent contemplates a scenario were MPC elements are installed on a destination device prior to loading the Downloadable. *See* '633 Patent, Fig. 11; *see also id.* at 19:65-20. Accordingly, the Court rejects Cisco's non-infringement arguments to the extent that they require the components Finjan identifies as MPC to be "transmitted" or "communicated."

With that in mind, the Court now turns to each accused components identified as MPC and the parties' arguments as to whether they are "executable" and "at runtime, monitor[] or intercept[] actually or potentially malicious code operations without modifying the executable code."

**3. Kernel Monitor**

Cisco does not contend in this motion that [redacted] (or analogous component in [redacted]) is not executable code or that it does not monitor or intercept actually or potentially malicious code operations without modifying the executable code. *See* MSJ at 11. Thus, Cisco's only non-infringement argument regarding kernel monitor is that it is "not

mobile" because "[redacted]d" and thus is not transmitted. MSJ at 15. Finjan responds that transmittal is not a requirement of claim 14 and even if it were, "Cisco's [redacted]' still infringes because it is necessarily transmitted when [redacted]" Opp'n at 14 (citing Expert Report of Nenad Medvidovic, Ph.D. Regarding Infringement By Cisco Systems, Inc. of Patent No. 7,647,633 ("Medvidovic Rpt.") ¶¶ 635, 659, ECF 400-8).

As the Court explained above, claim 14 does not require MPC to be transmitted or communicated. Accordingly, the Court DENIES Cisco's motion for summary judgment as to kernel monitor.

**4.** [redacted]

As for the remaining accused components, Cisco argues that Finjan fails to demonstrate that they satisfy both requirements for the claimed MPC – specifically, that they (1) are executable and (2) monitor or intercept actually or potentially malicious code operations without modifying the executable code. *See* MSJ at 15-16. Finjan responds that "[e]ach identified MPC is used to create and generate the virtual machines, which are used to monitor and intercept malicious computer operations resulting in a report, thereby comporting with the Court's construction of MPC." Opp'n at 15. Finjan goes on to cite to its expert's report, Cisco's internal documents, and various technical depositions to describe each of the accused components and why they satisfy the MPC requirements. *See* Opp'n at 15-18. Cisco's main objection to Finjan's theory is that even if "these [accused] items can configure, generate or create a [redacted], the claim requirements are not satisfied because the ***MPC itself*** must be the executable code that at runtime monitors/intercepts actual or potentially malicious code operations (as construed by the Court). Reply at 9. Cisco insists that it is the [redacted] that does the monitoring. *Id.* Finjan concedes that the accused components themselves do not monitor – but argues that they [redacted] Hr'g Tr. at 108:6-13

The Court is not persuaded that Finjan's theory is inconsistent with the Court's construction of MPC. To be sure, Finjan's theory appears to be one step removed from MPC as construed – but the Court's construction did not specify (and the parties did not ask the Court to do so) ***how*** the MPC monitors or intercepts malicious code. A reasonable jury may find that the accused components monitor or intercept malicious code [redacted] – satisfying the requirements for MPC. That said, the Court has reviewed the voluminous (and largely unhelpful) evidence cited by Finjan to determine whether it has pointed to ***any*** evidence that when viewed in the light most favorable to Finjan, would create a triable issue of fact regarding the [redacted] The Court's analysis for each component is summarized below.

[redacted] Finjan cites to testimony from Cisco's fact witness, Dean de Beer, and argues that [redacted] Opp'n at 15 (citing Transcript of Videotaped Deposition of Dean de Beer ("de Beer Dep.") at 69:11-20, ECF 400-18 [redacted]). Cisco concedes that [redacted]. MSJ at 15. Cisco also agrees that [redacted] Reply at 9. Accordingly, the Court is persuaded that a reasonable jury could agree with Finjan that [redacted] and thus satisfies the requirements for MPC.

[redacted] Finjan cites to an internal Cisco presentation and argues that [redacted] Opp'n at 16 (citing ECF 400-20 at CISCO-FINJAN_00204768.0004). The cited Cisco presentation states that [redacted] ECF 400-20 at CISCO-FINJAN_00204768.0004. Finjan fails to explain what [redacted]. The remaining string cited evidence also fail to shed any light as to how [redacted]

[redacted]. Accordingly, the Court finds that Finjan has failed to identify any triable issues of fact as to [redacted]. None of Finjan's cited evidence supports Finjan's assertion that [redacted] *See* Opp'n at 16. For example, Finjan cites to Cisco's fact witness testimony, reproduced below:

[redacted]

de Beer Dep. at 72:5-8. Finjan also cites to Dr. Medvidovic's report, where he identifies [redacted] as MPC without any explanation. *See* Medvidovic Rpt at ¶ 4332. The cited testimony from Mr. Brozefsky's deposition (another Cisco fact witness) and the cited internal Cisco document appear to be describing the overall architecture of Threat Grid and [redacted] – and it is unclear (and Finjan fails to explain) how they relate to application launch scripts or whether application launch scripts create virtual machines – let alone monitor or intercept anything. *See* Transcript of Videotaped Deposition of Craig Brozefsky ("Brozefsky Dep.") at 24:16-25:8, ECF 400-32; ECF 400-26 at CISCO-FINJAN_00074535.00010, 19, 20. The Court is not persuaded that Finjan has identified any material triable issue of fact with respect to [redacted] Finjan has failed to cite to evidence to support that [redacted] Finjan appears to be citing to evidence describing [redacted] (not accused as MPC) instead of [redacted]" (accused as MPC). *See* Medvidovic Rpt ¶ 4332 (identifying [redacted] as MPC and [redacted] as "mobile code executor"). The cited testimony from Mr. Brozefsky identifies [redacted] Brozefsky Dep. at 38:16-20. This is consistent with Mr. Brozefsky declaration that [redacted] Declaration of Craig Brozefsky in Support of Cisco Systems, Inc.'s Motion for Partial Summary Judgment ("Brozefsky Decl.") ¶ 10,

ECF 382-11. The Court is not persuaded that Finjan has identified any material issues of fact as to whether [redacted] (a data structure) is executable code – a requirement for MPC under the Court's construction.

[redacted] Finjan simply argues that [redacted] is "executable code because it is in the [redacted] programming language and monitor or intercepts potentially malicious computer operations by creating a virtual environment in [redacted] Opp'n at 17 (citing Medvidovic Rpt ¶ 4341, ECF 400-34 at CISCO-FINJAN_00000721.0002). The cited evidence, however, does not support Finjan's assertion. The cited Cisco document provides:

[redacted]

ECF 400-34 at CISCO-FINJAN_00000721.0002. Dr. Medvidovic references the same Cisco document and makes no mention of creating a virtual environment. *See* Medvidovic Rpt ¶ 4341. Finjan has not pointed to any evidence that [redacted] is executable code or that it creates a virtual environment. Thus, Finjan has failed to identify a triable issue of fact as to [redacted]

[redacted] Finjan argues that [redacted] Opp'n at 17 (citing Medvidovic Rpt.¶ 461). Finjan further argues that [redacted] lly [redacted] Opp'n at 18 (citing 400-36 at CISCO-FINJAN_00272162.0008). Cisco does not meaningfully dispute Finjan's claims but argues that Finjan has no evidence that the commands actually used in Cisco's [redacted] (as opposed to the general universe of commands noted in the [redacted] Finjan cites) are those that Finjan relies on. Reply at 11. Cisco might be correct – but the dispute is a factual one and not properly subject to summary judgment.

***

For the reasons stated above, the Court GRANTS Cisco's motion for summary judgment as to [redacted]" accused as MPC. The Court DENIES Cisco's motion for summary judgment as to [redacted]

**5. Estoppel under Doctrine of Equivalents**

"[P]rosecution history estoppel limits the broad application of the doctrine of equivalents by barring an equivalents argument for subject matter relinquished when a patent claim is narrowed during prosecution." *Conoco, Inc. v. Energy & Envtl. Int'l, L.C.*, 460 F.3d 1349, 1363 (Fed. Cir. 2006). The Federal Circuit recognizes that "prosecution history estoppel can occur during prosecution in one of two ways, either (1) by making a narrowing amendment to the claim ('amendment-based estoppel') or (2) by surrendering claim scope through argument to the patent examiner ('argument-based estoppel')." *Id.* Cisco argues that both occurred here. As an initial matter, the Court notes that the briefing on this issue is sparse. For example, it is unclear which specific DOE theories Cisco seeks to preclude under the amendment-based estoppel theory. In any event, the Court endeavors to address the issues presented.

First, Cisco argues that "all claims originally submitted by Finjan were rejected, and then Finjan amended each limitation to which it now applies the DOE." MSJ at 16. According to Cisco, because "claim 14 was narrowed by amendment for a reasons related to patentability (to overcome the prior art and 101 rejections), there is a presumption that DOE is not available to claim 14[.]" Reply at 12. Finjan responds that "amendments did not introduce new components nor change the scope of the claims" and therefore "there was no surrendering of scope." Opp'n at 20.

Where claims are amended, "the inventor is deemed to concede that the patent does not extend as far as the original claim," and the patentee has the burden of showing that the amendment does not surrender the particular equivalent in question. *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.*, 535 U.S. 738, 740 (2002). To succeed, then, the patentee must establish that: (1) the equivalent was unforeseeable at the time the claim was drafted; (2) the rationale underlying the amendment bears no more than a tangential relation to the equivalent in question; or (3) the patentee could not reasonably be expected to have described the insubstantial substitute in question. *Id.* at 740–41.

The amendments to claim 14 (claim 30 at prosecution) are reproduced below:

> **30.** (currently amended) A computer program product, comprising a computer usable medium having a computer readable program code therein, the computer readable program code adapted to be executed for computer security, the ~~processor-based~~ method~~,~~ comprising:
>
> providing a system, wherein the system comprises distinct software modules, and wherein the distinct software modules comprise an information re-communicator and a mobile code executor;
>
> receiving, at ~~an~~ the information re-communicator, downloadable-information including executable code; and
>
> causing mobile protection code to be executed by [[a]] the mobile code executor at a downloadable-information destination such that one or more operations of the executable code at the destination, if attempted, will be processed by the mobile protection code.

ECF 378-19 at FINJAN-CISCO 000890 (amendments underlined and struck through). This amendment was in response to the Office Action dated February 25, 2009, where the examiner rejected claim 14 (claim 30 at prosecution) under 35 U.S.C. § 101 and under 35 U.S.C. 102(e) as being anticipated by Golan, U.S. Patent 5,974,549. *See* ECF 378-18 at FINJAN-CISCO 000910, 11. "If a claim is narrowed for any reason related to patentability, 'the inventor is deemed to concede that the patent does not extend as far as the original claim.'" *Quintal Research Grp., Inc. v. Nintendo of Am., Inc.*, No. C 13-00888 SBA, 2015 WL 4396464, at *11 (N.D. Cal. July 17, 2015) (quoting *Festo*, 535 U.S. at 722, 737-38). Thus, a narrowing amendment may occur when a preexisting claim limitation is narrowed by amendment or when a new claim limitation is added by amendment. *AngioScore, Inc. v. TriReme Med., Inc.*, 50 F. Supp. 3d 1276, 1301 (N.D. Cal. 2014) (citation and quotation marks omitted). Here, the overall claim was narrowed because claim limitations were added. Accordingly, the Court agrees with Cisco that the amendment was a narrowing one to overcome a patentability challenge.

Next, the Court must consider whether Finjan has rebutted the presumption that it surrendered the equivalent in question. Cisco has not identified the specific equivalent for which it seeks summary judgment. To the extent Cisco is arguing that Finjan's amendment surrendered equivalents of MPC – due to the rejection based on the Golan reference – the Court is not persuaded.

Finjan argues that the amendments were not due to the Golan reference because "Finjan identified the same claim element that existed before the amendment (and, aside from the grammatical change after the amendment) as not being taught by Golan and the examiner agreed." Opp'n at 20 (citing ECF 378-17 at FINJAN-CISCO 001021). The Court agrees. The element that contains the MPC limitation had no more than a grammatical change and thus the amendment bears "no more than a tangential relation" to the MPC element. *See Festo*, 535 U.S. at 740. Moreover, it appears that Finjan overcame the Golan rejection by argument – not by amendment. Thus, the Court DENIES Cisco's motion for summary judgment on the basis of amendment-based estoppel of Finjan's DOE theories regarding MPC. To the extent that Cisco seeks summary judgment on other DOE theories (unrelated to MPC) the Court finds that the issue is not adequately briefed and declines to rule on it.

Second, Cisco argues that "Finjan is estopped by argument-based estoppel" because "Finjan argued clearly and unmistakably during prosecution that its invention was different from the Golan reference because 'Golan discusses a situation whereby a security monitor is already resident on a client computer.'" MSJ at 17 (citing ECF 378-17 at FINJAN-CISCO 001020; ECF 378-19 at FINJAN-CISCO 000899). Thus, according to Cisco, "by asserting a theory whereby a file is transmitted to an alleged Information-Destination where there is 'already resident' something Finjan characterizes as MPC, Finjan attempts to recapture through DOE exactly what it distinguished by argument during prosecution, which it cannot do." MSJ at 17. Finjan responds that Cisco's argument-based estoppel theory is "an attempt to reargue claim construction of 'mobile protection code.'" Opp'n at 20. Finjan also argues that there was no "clear and unmistakable surrender of subject matter" during prosecution. Opp'n at 19.

The Court agrees with Finjan that Cisco's argument-based estoppel theory is an attempt to relitigate the claim construction of "mobile protection code" – where Cisco's efforts to include "mobile" in the construction were unsuccessful. *See* Cisco's Responsive Claim Construction Brief at 1 (citing to prosecution history distinguishing "present invention" from non-mobile, pre-installed protection code at the client), ECF 154 ; *see also Markman* Order II at 4-6. As the Court explained earlier in this Order, the Court is not persuaded that revisiting claim construction is warranted.

***

Accordingly, the Court DENIES Cisco's motion for summary judgment on DOE theories regarding MPC.

**D. Non-infringement of the '780 Patent**

**1. Background of the '780 Patent**

The '780 patent is directed to a system and a method "for protecting a computer and a network from hostile Downloadables." '780 Patent at 1:30-33. Downloadables are executable programs typically requested by Internet browsers or web engines. *Id.* at 1:50-55. Examples of Downloadables include Java applets, JavaScript scripts, and ActiveX controls. *Id.* at 1:55-61. The specification explains that computer network security systems "are not configured to recognize computer viruses which have been attached to or configured as Downloadable application programs." *Id.* at 1:47-50. To that end, the '780 patent involves: (1) a security policy, (2) an interface for receiving a Downloadable, and (3) a comparator "for applying the security policy to the Downloadable to determine if the security policy has been violated." *Id.* at 2:1-4. Once the system receives a Downloadable, the system uses an ID generator to compute a Downloadable ID by fetching all the components of the Downloadable and performing a hash function on the Downloadable and the fetched components. *Id.* at 2:12-16. Next, a security policy may indicate which test to perform on the Downloadable, including:

> (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trust certificates; and (5) a comparison of the URL from which the Downloadable originated against trust and untrusted URLs.

*Id.* 2:17-26. A local engine will then determine, based on the result of these comparisons, whether to allow or block the Downloadable. *Id.* 2:26-27.

The only asserted independent claim (claim 9) provides:

> 9. A system for generating a Downloadable ID to identify a Downloadable, comprising:
>
> > a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable; and

> an ID generator coupled to the communications engine that fetches at least one software component identified by the one or more references, and for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

'780 Patent, Claim 9.

The Court construed "performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID" to mean "performing a hashing function on the Downloadable together with its fetched software components to generate a unique and reproducible ID for that Downloadable." *Markman* Order I at 25. Relevant to this motion, the Court has found that the ID generator may perform "one or more" hashing functions to generate "one or more" Downloadable IDs for "one or more" Downloadables. *Id.*

**2. AMP Products**

Cisco argues that it is entitled to summary judgment as to the AMP products because AMP Products hash each file as received and thus, "Finjan cannot satisfy the 'fetched' requirement or the 'together' requirement of the Court's construction." MSJ at 19. Cisco explains [redacted] *Id.* On the other hand, [redacted]" *Id.*

Finjan does not meaningfully dispute that AMP Products hash files as received, but argues that software components that are "resident in a Downloadable" may nonetheless be "fetched" as required by the claims. Opp'n at 21. According to Finjan, "Dr. Mitzenmacher provided an opinion for each of the accused products (including AMP Products, Cisco Sandboxes, and combinations thereof) discussing 'hashing HTML files together with JavaScript' showing that the accused products for the '780 Patent infringe because the referenced software components (e.g., JavaScript), that may be 'inside' the Downloadable (e.g., HTML or web page) are ***fetched first*** in order for them to ***then be hashed together***." Opp'n at 21.

Cisco replies that (1) "[a]ll of Finjan's 'AMP' evidence describes what Threat Grid does

after it receives a file (a Downloadable) from AMP" and not the AMP Products on their own and (2) the claims require "'fetching' something that is not already in the Downloadable." Reply at 12-13.

As for Cisco's first argument, the Court has reviewed the specific cites Finjan provided with regard to AMP Products (Opp'n at 21-11 (citing Mitz. Rpt ¶¶ 1295, 1370, 1374, 1394, 1501, 1304))[7] and has identified one paragraph in which Dr. Mitzenmacher opines that the AMP Products hash files and internal software components together:

[redacted]

Mitz. Rpt ¶ 1394. Accordingly, Cisco's "no evidence" theory fails.

As for Cisco's substantive argument, the Court finds that Finjan has identified a disputed issue of fact. Specifically, Finjan's expert opines that an internal software component may be "fetched" – and Cisco disagrees. Cisco dubs the dispute as "a question of claim construction." Reply at 13 (citing prosecution history and written description of the '780 Patent). The Court disagrees. The parties do not dispute that fetching must occur – Cisco simply rejects Dr. Mitzenmacher's opinion that software components may be fetched from within a Downladable.

> Q. So your opinion is that a downloadable that contains components when downloaded by a device, that device would also be fetching the components that are within that downloadable?
>
> A. I'd say that would be one way that it could occur.

Deposition of Michael Mitzenmacher at 210:11-16, ECF 400-48. Moreover, as Finjan pointed out at the Hearing, the '780 Patent contemplated the scenario where the software components are "embodied" in the Downloadable:

[7] To be clear, the Court has not (or could reasonably be expected to have) reviewed the 600+ pages of Finjan's expert report as suggested by Finjan's string cites. *See* Opp'n at 20 (citing Mitz. Rpt ¶¶ 820-1635).

> The ID generator **315** preferably prefetches all components embodied in or identified by the code for Downloadable ID generation. For example, the ID generator **315** may prefetch all classes embodied in or identified by the Java TM applet bytecode to generate the Downloadable ID.

'780 Patent, 4:56-61; Hr'g Tr. at 147:6-9 ("Mr. Hannah: The specification in column 4, line 56, it actually specifically addresses this issue in which components are embodied within the Downloadable. The Software components are embodied in the Downloadable.")

***

Accordingly, viewing the evidence in the light most favorable to Finjan, the Court finds that a material issue of fact exists and thus DENIES Cisco's motion for summary judgment as to AMP Products.

**3. Threat Grid and [redacted]**

Cisco seeks summary judgment of non-infringement as to Threat Grid and [redacted] on the ground that Finjan identifies no evidence that Threat Grid and [redacted] perform a hashing function on the Downloadable and fetched software components ***together***. MSJ at 20. As for Threat Grid, Cisco explains that when a file ("sample") is submitted, Threat Grid generates [redacted]. MSJ at 20 (citing Brozefsky Decl. ¶ 12). Threat Grid may then execute the sample in a sandbox, which may result in "artifacts" being created and after the execution is completed [redacted]. MSJ at 20 (citing Brozefsky Decl. ¶¶ 13-14). Based on this description, Cisco argues that "[w]hile the hashes of the [redacted] ultimately may be stored together, they are not hashed together[.]" MSJ at 20. As for [redacted], Cisco argues that Finjan has only identified "an analysis report generated by [redacted] that includes a number of hashes" but has no evidence that [redacted] performs a hashing function on the Downloadable and fetched software components together." MSJ at 20. According to Cisco, summary judgment is warranted because "a 'collection of hashes' is not a Downloadable ID." MSJ at 20 (citing Mitz. Rpt ¶¶ 1365-1366, 1400-1402, 1528-1530).

Finjan responds that its infringement theories demonstrate that Cisco's products "fetch" and "hash" files "together." Opp'n at 21. First, Finjan asserts that Dr. Mitzenmacher provided an

opinion for Cisco Sandboxes (like he did for AMP Products) [redacted] showing that the accused products for the '780 Patent infringe because the referenced software components [redacted] that may be 'inside' the Downloadable (*e.g.*, HTML or web page) are ***fetched first*** in order for them to then be ***hashed together***." *Id.*; *see also* Opp'n at 22 (citing Mitz Rept ¶¶ 1370, 1374). As the Court concluded above for AMP products, Finjan has identified a material issue of fact as to whether software components may be "fetched" from "inside" the Downloadable.

Second, Finjan argues that Threat Grid and [redacted] hash the Downloadable and the fetched software components together because "a file will be hashed together with its fetched software components and the combined analysis will include a unique Downloadable ID [redacted]." Opp'n at 22 (citing Mitz. Rpt ¶¶ 1295, 1299, 1330, 1335, 1339, 1344, 1361, 1365, 1381, 1400). The cited paragraphs, however, support Cisco's explanation that the file and its components are [redacted]. Finjan's counsel confirmed at the Hearing that [redacted] as it comes in to Cisco's sandboxes and those hashes are then put in a report:

> Mr. Hannah: …. It's a single session they call. And so the file comes in, [redacted] That is all recorded in the same session. All of that is done together. Once that session is complete, ... and when they see the processing is done, then they spit out, as counsel said, a report.

Hr'g Tr. at 133:22-133:7. Finjan nonetheless claims that "these [redacted] are happening together because it's happening in a single session" [redacted]. Hr'g Tr. at 144:8-11.

The Court finds Finjan's "sequence of hashes" argument unpersuasive. The storing together of separately generated hashes does not satisfy the "together with" requirement of claim 9, as construed by the Court. First, Finjan's theory that the "sequence of hashes" are "happening together" because they take place in the "same session" appears nowhere in the cited expert testimony. Second, the claim requires "performing a hashing function on the Downloadable ***together with*** its fetched software components to generate a unique and reproducible ID for that

Downloadable." *Markman* Order I at 25. The Court fails to see how a "sequence of hashes" (created in one session or otherwise) stored in a file or report is any different than simple hashing of files and storing them together – neither of which Finjan invented. To be clear, the Court recognizes that under the Court's construction, the ID generator may perform "one or more" hashing functions – but that doesn't change the "together with" requirement, for which Finjan has failed to set forth any evidence. Accordingly, the Court concludes that Finjan's theory of "sequence of hashes" stored in a file or report does not satisfy the claim requirements.

***

Accordingly, with respect to Threat Grid and [redacted], the Court (i) DENIES summary judgment as to Finjan's infringement theory that software components may be fetched from "inside" the Downloadable and then hashed together with the Downloadable and (ii) GRANTS summary judgment as to Finjan's infringement theory that a "sequence of hashes" stored in a report or file satisfies the "together with" requirements of claim 9.

**4. Dropper (Dropped Filed)**

Separately, Cisco challenges Finjan's infringement theories with regard to dropper (or dropped) files. Cisco explains that dropped files are downloaded in response to a first file being executed. MSJ at 22. Cisco argues that "dropped files" are "separate executable files that are downloaded as a result of the original (*e.g.*, 'parent') file executing" and thus, cannot satisfy the claim element "software components required to be executed by the Downloadable." MSJ at 22. To make this argument, Cisco relies on the nature and functionality of dropper (or dropped) files, but cites to no evidence in support of its factual assertions. Finjan, on the other hand, cites to Dr. Mitzenmacher's report, in which he describes the operation of dropper (or dropped) files within Threat Grid. Opp'n at 23. On this record, the Court declines to conclude that no material dispute of fact is present and DENIES summary judgment with respect to dropper (or dropped) files on the ground that dropper (or dropped) files are "separate executable files."

**5. Estoppel under Doctrine of Equivalents**

Cisco seeks summary judgment on Finjan's DOE infringement theory for the ID generator limitation of claim 9 (claim 11 at prosecution). Cisco argues that the ID generator limitation was

amended during prosecution to distinguish prior art by affirmatively requiring the ID generator to fetch at least one software component and to perform a hashing function on the Downloadable and the fetched software components. MSJ at 22 (citing ECF 378-14 ('780 Patent File History) at FINJAN-CISCO 000577, 602, 609). Because the amendments to claim 9 narrowed the scope of the claim for purposes of patentability, Cisco argues, Finjan is estopped from asserting a DOE theory on this element. MSJ at 22. Finjan responds that the amendment only "reworded" the claim language and did not narrow the scope of the claim because the "fetching" and "hashing" language was included in the claim prior to the amendment. Opp'n at 24. According Finjan, because the amendments were not made "to narrow the claim element to overcome prior art, the ID generator is not subject to prosecution history estoppel." *Id.*

Claim 9 (claim 11 during prosecution) was amended twice, as demonstrated below:

> 11. (Currently amended) A system for generating a Downloadable ID to identify a Downloadable, comprising:
>
> a communications engine for obtaining a Downloadable that includes one or more references to software components required by the Downloadable; and
>
> an ID generator coupled to the communications engine for fetching[, if the Downloadable includes one or more references to a component,] at least one software component identified by the one or more references, and for performing a function on the Downloadable and [all] the fetched software components [fetched] to generate a Downloadable ID.

ECF 378-14 at FINJAN-CISCO 000577 (amendments underlined).

9
~~11~~. (Currently amended) A system for generating a Downloadable ID to identify a Downloadable, comprising:

a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable; and

an ID generator coupled to the communications engine ~~for fetching~~ that fetches at least one software component identified by the one or more references, and for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

ECF 378-14 at FINJAN-CISCO 000602 (amendments in handwriting).

Here, contrary to Finjan's assertion, the amendment did not simply reword the claim language. The ID generator element was amended to require: (1) fetching of at least one ***software*** component (as opposed to the broader pre-amendment language requiring fetching "at least one component") and (2) the claimed "function" to be a ***hashing*** function. These are narrowing amendments – triggering the amendment-based estoppel on Finjan's DOE theories regarding ID generator.

Moreover, the amendments were made to overcome patentability challenges. The examiner explained that the amended claim was allowed because "[i]t was not found to be taught in the art of a downloadable that includes references to software components required to be executed by the downloadable and performing a hashing function on the downloadable and the fetched software component to generate a downloadable ID." ECF 378-14 at FINJAN-CISCO 000610. Even if the examiner had not identified the amendments as the reason for allowance, when the record lacks explanation for the amendment, courts "presume that the PTO had a substantial reason related to patentability for including the limiting element added by amendment." *Conoco*, 460 F.3d at 1363 (citation omitted).

The burden then shifts to Finjan to show that the amendment does not surrender the particular ID generator equivalent in question. *Festo*, 535 U.S. at 740. Finjan argues that "'a function on the Downloadable and all components fetched to generate a Downloadable ID' as well as wherein the

function includes a hashing function' existed prior to any amendments." Opp'n at 24 (citing to ECF 378-14 at FINJAN-CISCO 000577-78). The Court is not persuaded. First, the "***software*** component" limitation was not included in the pre-amendment language. Second, the "***hashing*** function" was included in a separate (dependent) claim – not claim 9 (claim 11 at prosecution). *See* ECF 378-14 at FINJAN-CISCO 000578 (claim 17).

Finally, Finjan argues that "the examiner, not Finjan, added the 'hashing' function, thus prosecution history estoppel does not apply because there was no clear and unmistakable disavowal by the patentee." Opp'n at 24-25. Finjan appears to be conflating the standard for argument-based estoppel (which Cisco has not moved on as to the ID generator) with amendment-based estoppel (which Cisco has moved on). *See Conoco*, 460 F.3d at 1364 ("Unlike amendment-based estoppel, we do not presume a patentee's arguments to surrender an entire field of equivalents through simple arguments and explanations to the patent examiner."). When applying amendment-based estoppel, courts "presume that the patentee surrendered all subject matter between the broader and the narrower language" when an amendment is made for purposes of patentability. *Festo*, 535 U.S. at 739.

In sum, Finjan has failed to articulate why the amendments to claim 9 do not surrender the DOE infringement theories it asserts. Accordingly, the Court GRANTS Cisco's motion for summary judgment on Finjan's DOE infringement theories as to the ID generator limitation of claim 9.

**E. Pre-Suit Damages**

Cisco seeks summary judgment on the issue of pre-suit damages because "[n]o admissible evidence exists of Finjan putting Cisco on notice, prior to the filing of the Complaint, that a specific Cisco product infringes a specific Finjan patent, as required under the law to recover pre-suit damages." MSJ at 23. Finjan concedes that "for purposes of this trial only and preserving all appeals, the start date of damages is the filing of the initial complaint on January 6, 2017." Opp'n at 25. Because there is no dispute, the Court GRANTS Cisco's motion for summary judgment and holds that Finjan is not entitled to recover damages prior to the date it filed suit (*i.e.*, January 6, 2017).

## IV. ORDER

For the foregoing reasons, the Court:

(1) As to Cisco's motion for summary judgment of non-infringement of the '154 Patent,

a. Cisco's motion is GRANTED with respect to AMP Products,

b. Cisco's motion is DENIED with respect to URL rewriting feature of the ESA Outbreak Filters, and

c. Cisco's motion is GRANTED with respect to [redacted] accused as "content processor."

(2) As to Cisco's motion for summary judgment of non-infringement of the '633 Patent,

a. Cisco's motion is GRANTED with respect to [redacted] accused as MPC,

b. Cisco's motion is DENIED with respect to kernel monitor, [redacted]" accused as MPC, and

c. Cisco's motion for summary judgment is DENIED with respect to Finjan's DOE theories regarding MPC.

(3) As to Cisco's motion for summary judgment of non-infringement of the '780 Patent;

a. Cisco's motion for summary judgment is DENIED with respect to AMP Products,

b. Cisco's motion for summary judgment with respect to Threat Grid and [redacted] is (i) DENIED as to Finjan's infringement theory that software components may be fetched from "inside" the Downloadable and then hashed together with the Downloadable and (ii) GRANTED as to Finjan's infringement theory that a "sequence of hashes" stored in a report or file satisfies the "together with" requirements of claim 9.

c. Cisco's motion for summary judgment is DENIED with respect to dropper (or dropped) files on the ground that dropper (or dropped) files are "separate executable files."

d. Cisco's motion for summary judgment is GRANTED with respect to Finjan's

DOE theories regarding the ID generator limitation of claim 9.

(4) Cisco's motion for summary judgment on the issue of pre-suit damages is GRANTED.

**IT IS SO ORDERED.**

Dated: March 20, 2020

BETH LABSON FREEMAN
United States District Judge